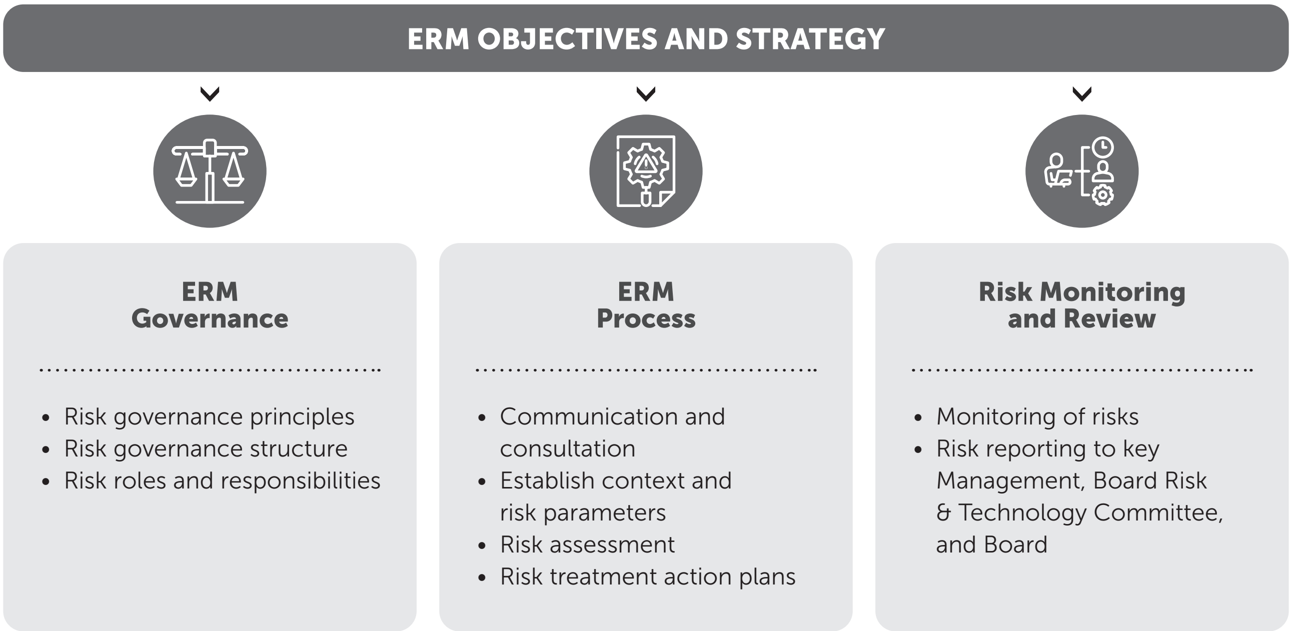
ENTERPRISE RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT (ERM) APPROACH

ERM Framework of the SingPost Group

The Group's ERM framework is modelled based on the ISO 31000:2018 Risk Management – Guidelines, and covers the key strategic, operational, financial, compliance, and information technology risks facing the Group. The ERM framework is supported by appropriate risk policies, procedures and provides guidance to the Group's various business units and support units on managing risks.



ERM OBJECTIVES AND STRATEGY

ERM Governance

- Risk governance principles
- Risk governance structure
- Risk roles and responsibilities

ERM Process

- Communication and consultation
- Establish context and risk parameters
- Risk assessment
- Risk treatment action plans

Risk Monitoring and Review

- Monitoring of risks
- Risk reporting to key Management, Board Risk & Technology Committee, and Board

ERM FRAMEWORK

RISK GOVERNANCE

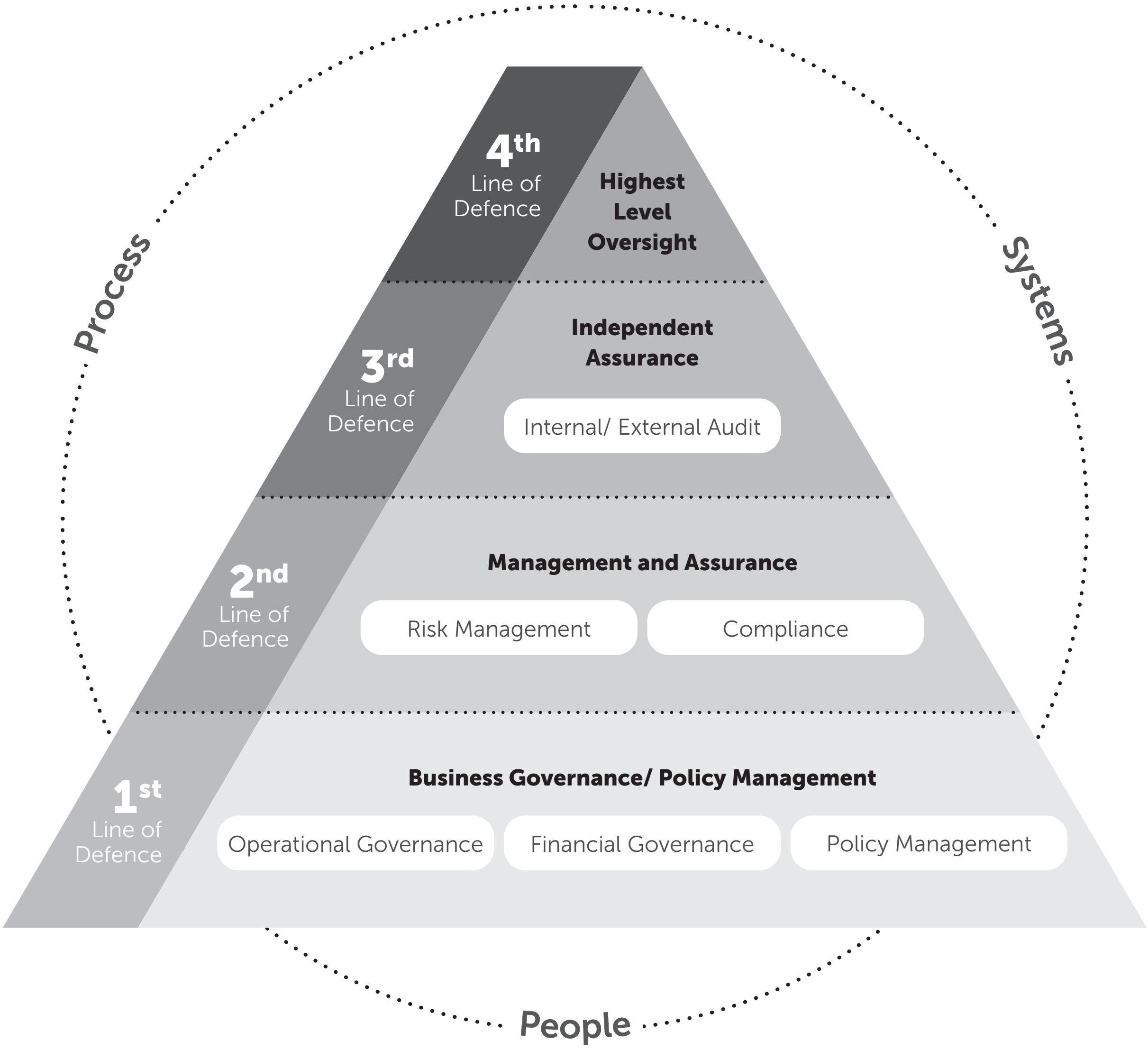
The Group's ERM programme and internal controls are reviewed on a regular basis and, where appropriate, refined by key Management with guidance from the Board Risk and Technology Committee (BRTC) and the Board.

The Board, through the BRTC, has overall responsibility for risk governance and ensures that the Group maintains a robust system of risk management and internal controls to safeguard stakeholders' interests and the company's assets and resources.

In addition, the BRTC sets the tone on the appropriate risk culture and provides guidance on the enterprise risk management system and the corresponding policies and procedures. The BRTC meets quarterly.

ENTERPRISE RISK MANAGEMENT

The purpose of risk governance is to embed and build on the four lines of defence (as illustrated in the diagram below), which is a prerequisite to promote a robust system of risk management and effective internal controls.

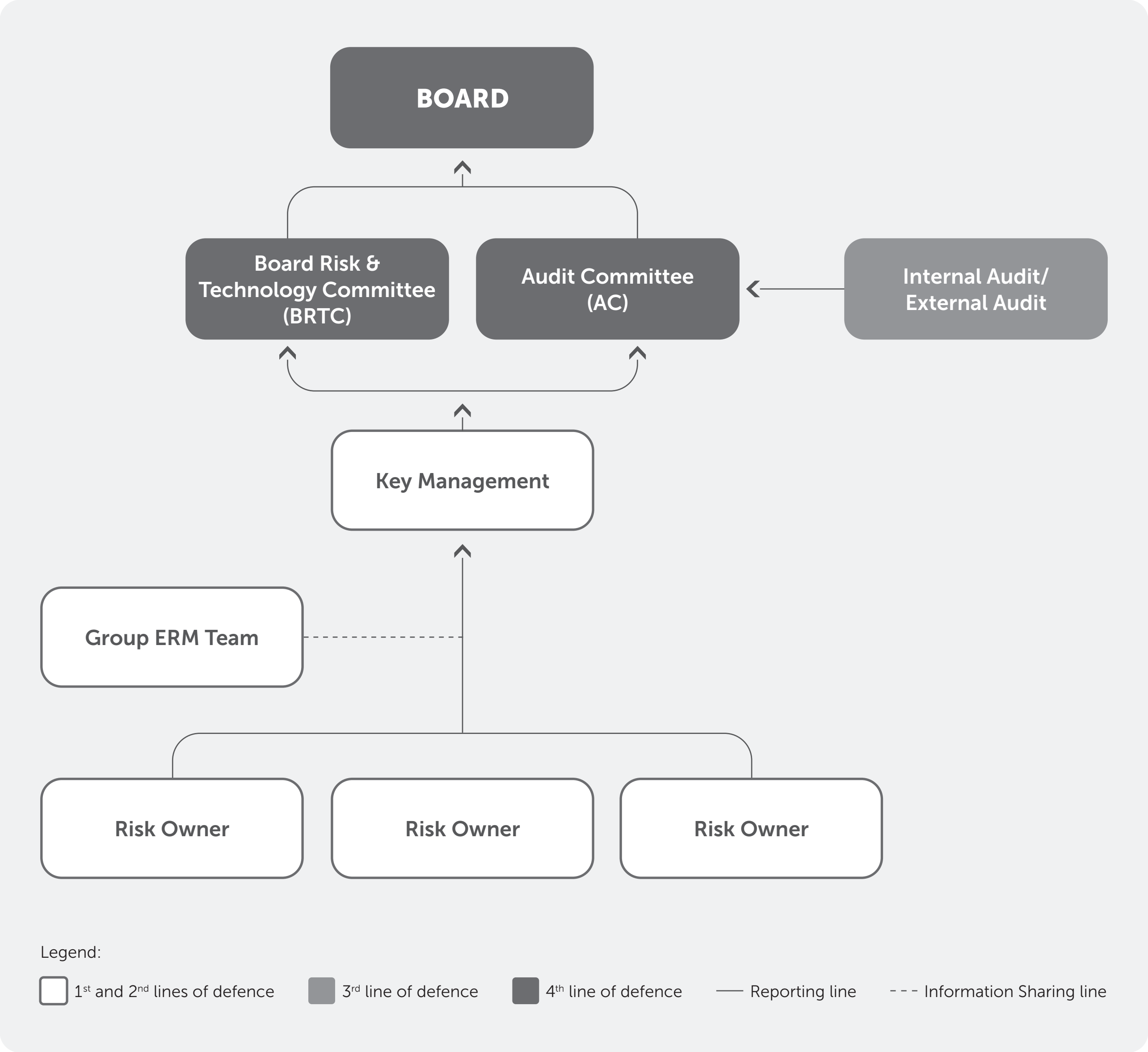


4 LINES OF DEFENCE

RISK GOVERNANCE STRUCTURE

The adoption of the above four lines of defence develops a risk governance structure. It embeds the Group's existing organisational structure with assigned risk roles and responsibilities.

ENTERPRISE RISK MANAGEMENT

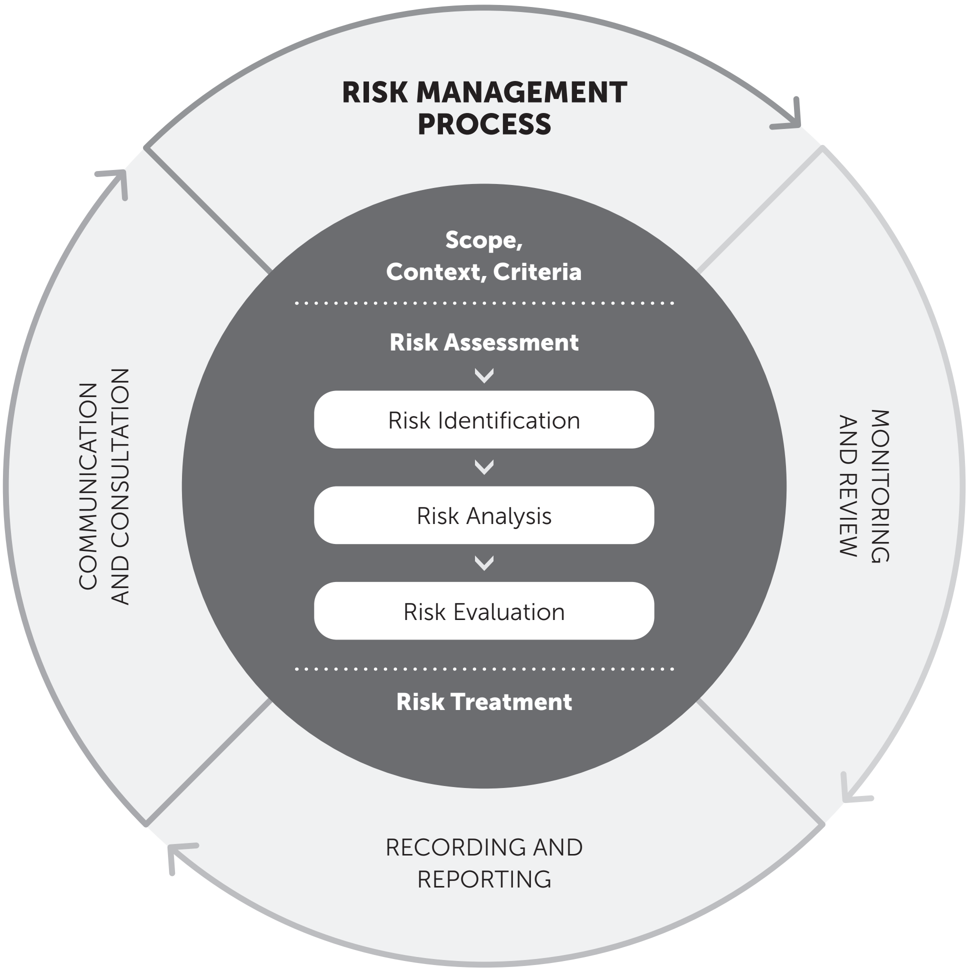


ERM PROCESS

The ERM process aims to achieve the following:

- A structured, disciplined and systematic approach to managing risks;
- Robustness of risk information;
- Accountability for outcomes and risk treatment action plans; and
- Sustainability.

ENTERPRISE RISK MANAGEMENT



RISK APPETITE STATEMENTS

The Group's risk appetite statement reflects the nature and extent of risks the Group is willing to take in pursuing its strategic objectives. The Board have reviewed the following risk appetite statements during the financial year ended 31 March 2024:

1. **STRATEGY**
   The Group is committed to upholding its reputation as a trusted organisation while placing customers at the core of its business. This will include investments into people, innovation, infrastructure, cyber, and data security to the benefit of all stakeholders.

2. **SUSTAINABILITY & GROWTH**
   The Group aims to strengthen its market position in Singapore and the rest of Asia Pacific by taking measured risks that balances risk and reward in line with its strategic objectives and initiatives. The Group will also proactively seek to diversify its business while actively managing its risks.

3. **FINANCIAL**
   The Group aims to deliver value to shareholders with sustainable profitable growth. The Group is committed to maintain a strong financial position and targets an investment grade credit rating with adequate liquidity to meet its operational and financing obligations and longer-term goals.

4. **PEOPLE**
   The Group aims to be an employer of choice where it engages, develops, grows, and rewards talent, apart from providing employees and stakeholders a safe and healthy work environment. The Group is committed to complying with laws and regulations of all countries in which it operates, and to conduct business with integrity, fairness and high ethical standards in all business dealings and relationships.

ENTERPRISE RISK MANAGEMENT

KEY MATERIAL RISKS TO THE GROUP

The Group categorises its risk profile into five key areas: **Strategic, Financial, Operational, Compliance, and Information Technology**.

STRATEGIC RISKS

A large part of the Group's strategic risks comprises market-driven forces, evolving business landscapes, changing customer demands, concentration of key customers, disruptive technology, and declining letter volume.

Risk Name	The Group manages by
Concentration (The Group recognises the risk of over-reliance on revenue generated by its business unit and its products.)	• Diversifying transshipment origin, trade lanes and destination countries. • Strengthening and optimising a regional transhipment hub to serve our eCommerce customers. • Developing and growing our Post and Parcel global transshipment hub to serve eCommerce customers (from Platforms to Brands). • Diversifying the Group's income streams to prevent over-reliance on a particular business unit.
Declining Letter Volume (The Group recognises the risk of technological advancements replacing physical letters, this poses a threat to the Group's revenue mix.)	• Focusing on the growth of eCommerce volume to mitigate e-substitution. • Improving process automation along with application of smart technologies in infrastructure to enhance efficiency.
Merger & Acquisition (The Group recognises the risk arising from the process of acquiring and integrating businesses.)	• Adopting a disciplined investment evaluation and decision process governed by the Group M&A policy. • Integrating the acquired businesses, as appropriate, to maximise synergies and to ensure compliance with corporate governance and reporting requirements. • Appointing members of the Group's management to the Boards of acquired businesses and/or appointing management team members, in order to transfer the Group's culture, values and processes to the acquired businesses.
Market Risk (The Group recognises that the logistics industry is an open and competitive one, with rising costs and increasing expectations for higher service standards. Failure to plan for the constantly evolving competitive landscape and grow required capabilities and networks would limit the Group's growth potential.)	• Developing multiple growth markets to diversify both sources and types of revenue. • Using data to analyse market outlook and formulate the enterprise strategy. • Establishing cost-efficient cross border hubs. • Enhancing our processing and network capacity to meet new demands.

ENTERPRISE RISK MANAGEMENT

FINANCIAL RISKS

The Group has diversified global businesses, partially funded by external debts in addition to shareholders' funds. This exposes the Group to liquidity risk, interest rate risk, and foreign currency risk. The Group has established policies, guidelines, and control procedures to manage and report exposure to such risks.

Risk Name	The Group manages by
Treasury (The Group's businesses and operations may be exposed to unfavourable movements in foreign exchange rates, interest rates, that may result in potential financial losses.)	**Liquidity Management** • Monitoring and maintaining a level of cash and cash-equivalents to finance operations and to mitigate the effects of fluctuations in cash flows. • Maintaining funding flexibility with credit facilities available to meet short-term obligations as they fall due. **Interest Rate** • Reviewing the Group's interest rate exposures on Group's debt obligations and interest-bearing financial assets. • Maintaining a prudent mix of fixed and floating interest rates for the outstanding borrowings or debts to manage fluctuations in the interest rate environment. • Placing cash balances with reputable banks and financial institutions with different maturities to manage interest income on different interest rate terms. **Foreign Currency** • Constantly reviewing foreign currency exposure from fluctuations arising from the Group's operations and subsidiaries, and associates in foreign countries. • Using a hedging framework, matching currencies, and hedging instruments to hedge known exposure from foreign currency exchange rate fluctuations.
Credit Management (The Group recognises that weak credit control management over customers, customers' slow payment or non-payments when customers' accounts receivables are due may result in potential significant bad debts.)	• Screening during onboarding and periodically reviewing the credit worthiness of customers. • Applying suitable credit terms on customers based on the credit risk exposure analysis on the latter. • Ensuring strict compliance of credit policy with deviations granted only on exceptional basis and in accordance with approved authorisation matrix. • Escalating outstanding receivables to key Management on monthly- and quarterly-basis. • Placing trade credit insurance to lower risk exposures.

ENTERPRISE RISK MANAGEMENT

OPERATIONAL RISKS

The Group's operations are exposed to a variety of operational risks relating to workplace safety and health, and talent retention.

Risk Name	The Group manages by
Environment, Health & Safety (The Group recognises the importance of taking reasonably practicable safety and health measures at its workplaces and business activities to prevent severe injury or death of staff and/or customers.)	• Establishing Environment, Health & Safety (EHS) policies and procedures to guide businesses on approach and expectations. • Regular monitoring, reviews and updates of WSH performance and improvement strategies at safety consultation forums/ safety committee meetings (where applicable), Management meetings, to Board Sustainability Committee and the Board • Collecting and reviewing observations and incident data, near misses; investigating incidents and mapping action plans for improvements and prevention. • Conducting safety awareness training, communications and workshops for employees. • Conducting EHS inspections at all workplaces to identify hazards and ensure compliance to relevant EHS laws and regulations.
Talent Retention (The Group recognises the importance of retaining personnel with key institutional knowledge, information, experience, skills, and connections for key positions in the SingPost management group to ensure operational effectiveness and business sustainability.)	• Robust approach to talent identification, assessment and development to provide a holistic organisational view of talent pipelines and bench strength. • Offering the identified pool of talent accelerated development opportunities that include formal learning, coaching and mentoring, as well as action learning projects, to enhance their skills and competencies. • Succession planning for key executive and critical roles identified across the business to raise awareness of and systematically mitigate risks arising from potential unavailability of talent. • Applying pay differentiation to encourage top performers.
Business Continuity (The Group recognises the importance and the need to recover from a business/ operational disruption quickly to minimise impact to our customers, operations and assets.)	• Establishing business continuity policies and procedures to respond to disruptive events. • Training personnel of the business continuity plans. • Reviewing and monitoring the effectiveness of the business continuity plans through annual exercises.

ENTERPRISE RISK MANAGEMENT

COMPLIANCE RISKS

The Group's business operations are exposed to a variety of compliance risks relating to postal regulations and associated government regulations.

Risk Name	The Group manages by
Data Privacy (The Group recognises that data privacy breaches may undermine customer confidence and may result in litigation from customers and/or be subject to regulatory fines and penalties.)	• Maintaining an accountability-based data privacy framework to work in conjunction with the IT security framework to safeguard personal data collected, processed, and disclosed. • Maintaining a governance structure to ensure oversight is provided by the Board and key Management on the adequacy and effectiveness of the Group's privacy programme and control measures. • Developing and implementing data privacy focused policies and procedures group wide. • Conducting regular mandatory training to all employees on the Group's data privacy framework and associated policies and procedures to create awareness and compliance. • Assigning clear lines of responsibilities to all employees to ensure adequate data governance across the Group.
Governance (Fraud, Bribery and Corruption) (The Group recognises that fraud, bribery and corrupt acts committed by employees/ officers and non-compliance with internal governance/ Standard Operating Procedures, may result in financial loss and/or reputation damage to the Group.)	• Maintaining a zero-tolerance policy and "tone from the top" towards fraud, bribery, and corruption. • Reviewing internal controls periodically and conducting training and awareness activities. • Mandating all staff to undergo the annual Code of Conduct declaration exercise where the anti-bribery and anti-corruption requirements are spelt out for compliance and affirmation. • Maintaining whistle-blowing escalation process where the Group Internal Audit independently manages and investigates whistleblowing incidents, and all whistle-blowing reports received are reported to the Audit Committee on a quarterly basis. • Embedding the Code of Ethics into the Code of Conduct policy to give emphasis on ethical behaviour and integrity of employees. • Maintaining a dedicated Ethics Committee at Management level to evaluate staff issues or concerns of an ethical nature, reviewing remediation and strengthening processes.
Payment Services Act ("PSA") (The Group is required to meet regulatory requirements for offering payment services under the PSA and notices and guidelines released by the Monetary Authority of Singapore. Non-compliance with the above may result in financial penalties or in the worst case, a suspension of the licence resulting in stoppage of the business.)	• Developing and implementing relevant policies and controls dealing with anti-money laundering and the financing of terrorism within the Group • Conducting comprehensive risks assessment to ensure compliance with the PSA regulations. • Conducting training to all employees on the applicable regulatory requirements of the PSA and associated policies and procedures to create awareness and compliance.

ENTERPRISE RISK MANAGEMENT

Risk Name	The Group manages by
Sanctions (The Group recognises that violations of trade compliance laws and regulations, including sanctions and embargoes, will carry fines and expose the Group and its employees to criminal sanctions and civil suits.)	• Monitoring and tracking the developments of significant sanctions issued by international organisations (e.g. United Nations) as well as unilateral sanctions issued by countries/jurisdictions such as the United States of America and the European Union. • Creating a continual awareness on the latest developments and requirements via monthly and ad-hoc email circulars to the various Business Units (BU) and Support Units (SU). • Establishing an escalation channel for BUs and SUs to flag any suspicious or high-risk transaction to Group Compliance for review and assessment and screen the associated parties against sanction lists/databases. • Applying the Third-Party Due Diligence policy to guide all employees on the required measures and process for due diligence when engaging third parties. • Monitoring and reviewing adequacy of resources for managing sanction risk to align with the evolving businesses and regulatory environment.
Postal Regulatory (The Postal Service is required to comply with the Postal Services Act, Postal Licence conditions, Postal Competition Code, Postal Services Regulations, Postal Services Operations Code, Quality of Service (QoS) standards for basic letters delivery services, and any Directions and Guidelines issued by the Infocomm Media Development Authority (IMDA). Non-compliance with the above may result in the imposition of financial penalties.)	• Having proactive and regular engagements with the Postal Regulator and other government agencies. • Conducting internal communications campaigns to train, educate and reinforce best behaviour. • Sending regular reminders to employees to comply with established protocols, guidelines, best practices, and directions, enhanced by strict disciplinary action taken for non-compliance. • Continually monitoring and assessing the impact of Postal Regulatory developments as the business evolves to minimise impact to the business.

INFORMATION TECHNOLOGY RISKS

With the increased reliance on information systems and technology as a business enabler, a service disruption of critical information technology (IT) systems or malicious and deliberate attempt of hackers to breach our IT systems could adversely affect the Group’s business continuity and reputation.

Risk Name	The Group manages by
IT Security (The Group recognises that cyber threats remain a key concern as attackers become increasingly creative with attack methods and may result in significant data losses.)	• Maintaining and continuously improving our IT security framework to address evolving IT security threats such as hacking, malware, and loss of data. • Dedicated IT security expertise to keep abreast on the latest developments, innovation, and threats in technology, and assessing their risks and impact.
Critical IT Systems Failure (The Group recognises that unplanned outage/downtime and/or performance deficiency of Critical IT systems may lead to negative customer experience, disruption to major operations, and/or regulatory actions or fines by the regulators.)	• Designing and implementing high availability IT systems, coupled with periodic testing for system validation. • Ensuring that IT servers are centrally and continuously monitored with appropriate escalations to be performed on any critical IT systems failure. • Monitoring mechanisms to mitigate poor performing critical systems.